



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|----------------------------------|-------------|----------------------|---------------------|------------------|
| 10/511,903 | 10/20/2004 | Junji Yoshida | 2004_1622A | 4793 |
| 513 | 7590 | 03/31/2009 | EXAMINER | |
| WENDEROTH, LIND & PONACK, L.L.P. | | | PHAM, LUU T | |
| 1030 15th Street, N.W., | | | ART UNIT | PAPER NUMBER |
| Suite 400 East | | | | 2437 |
| Washington, DC 20005-1503 | | | | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 03/31/2009 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | | |
|------------------------------|------------------------|---------------------|--|
| Office Action Summary | Application No. | Applicant(s) | |
| | 10/511,903 | YOSHIDA ET AL. | |
| | Examiner | Art Unit | |
| | LUU PHAM | 2437 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12/23/2008.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 13-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 13-15 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application

6) Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 12/23/2008.
2. In the instant Amendment, Claims 1-12 were previously canceled; Claims 13-15 have been amended; Claim 13 is independent claim. Claims 13-15 have been examined and are pending. **This Action is made FINAL.**

Response to Arguments

3. The objections to claims 13-15 are withdrawn as the claims have been amended.
4. The rejections of claims 13-15 under 35 U.S.C. § 101 are withdrawn as the claims have been amended.
5. The rejections of claims 13-15 under 35 U.S.C. § 112 second paragraph are withdrawn as the claims have been amended.
6. Applicants' arguments with respect to claim 13-15, regarding the limitation "*issuing Nth CA information that includes an Nth CA certificate indicating that the Nth server certificate is valid and include an (N+1)th address for update indicating a location of the (N+1)the download server,*" have been fully considered but they are not persuasive.

Applicants' arguments:

- a. Kenichi fails to disclose or suggest "*issuing Nth CA information that includes an Nth CA certificate indicating that the Nth server certificate is valid and include an (N+1)th address for update indicating a location of the (N+1)the download server.*"

The Examiner disagrees for the following reasons:

- a. Kenichi does disclose issuing N^{th} CA information that includes an N^{th} CA certificate indicating that the N^{th} server certificate is valid and include an $(N+1)^{th}$ address for update indicating a location of the $(N+1)$ the download server (*pars. 0011, 0014, 0017, and 0220; Fig. 4; certification authority address information 402; when the renewal program 102 of a certificate is started, according to the certificate authority address information 402 of the certificate 101, it will take connection 505 for the certificate authority 105 via a network*).
7. Applicants' arguments with respect to claims 13-15, regarding the limitation "starting up the $(N+1)^{th}$ authentication apparatus and the $(N+1)$ the download server," and "terminating the operation of the $(N+1)^{th}$ download server," have been considered but are moot in view of the new ground(s) of rejection.

Priority

8. Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d), a certified English translation of the foreign application must be submitted in reply to this action. 37 CFR 41.154(b) and 41.202(e).

Failure to provide a certified translation may result in no benefit being accorded for the non-English application.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

11. **Claims 13-15 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Kenichi et al., (hereinafter “Kenichi”), J.P. Patent Publication No. JP 2002-215826 published on August 02, 2002, in view of Perlman et al., (hereinafter “Perlman”), U.S. Patent No. 6,230,266 issued on May 08, 2001.

- **Regarding claim 13**, Kenichi discloses a method of operating a communication system comprising (i) an N^{th} authentication apparatus, (ii) an $(N+1)^{\text{th}}$ authentication apparatus, and an $(N+1)^{\text{th}}$ download server, each being connected over a communication network, wherein N and $(N+1)$ are values each indicating a number in a sequence in a case

where a plurality of authentication apparatuses and a plurality of corresponding download servers are sequentially put into operation, N being an integer of 1 or larger (*pars. 0007 and 0019-0020; Fig. 8; certificate authority A 801, certificate authority B 803, and computer 100*),

wherein the Nth authentication apparatus (*Fig. 8, certificate authority A 801*) includes:

an Nth server certificate issue unit operable to issue an Nth server certificate ensuring validity of an application server (*pars. 0019-0023; certificate 804*); and
an Nth certificate authority (CA) information issue unit operable to issue Nth CA information including an Nth CA certificate and an (N+l)th address for update, the Nth CA certificate indicating that the Nth server certificate is valid, and the (N+l)th address for update indicating a location of the (N+ 1)th download server on the communication network (*pars. 0007, 0011-0012, and 0014-0020; Figs. 4-9; certification authority address information 402*),

wherein the (N+ 1)th authentication apparatus (*Fig. 8; certificate authority B 803*) includes:

an (N+l)th server certificate issue unit operable to issue an (N+l)th server certificate ensuring the validity of the application server (*Fig. 8; certificate authority B 803*); and

an (N+ 1)th CA information issue unit operable to issue (N+ 1)th CA information including an (N+l)th CA certificate and an (N+2)th address for update, the (N+l)th CA certificate indicating that the (N+l)th server certificate is valid, the (N+2)th

address for update indicating a location, on the communication network, of an (N+2)th download server on which (N+2)th CA information is placed, and the (N+2)th CA information including an (N+2)th CA certificate to be a next valid CA certificate in a case where the (N+1)th CA certificate becomes revoked (*pars. 0007, 0011-0012, and 0014-0020; Figs. 4-9; certification authority address information 402; when the renewal program 102 of a certificate is started, according to the certificate authority address information 402 of the certificate 101, it will take connection 505 for the certificate authority 105 via a network*),

wherein the (N+ 1)th download server (*Fig. 8; computer 100*) includes:
a CA information storage unit operable to store the (N+ 1)th CA information including the (N+1)th CA certificate to be a next valid CA certificate in a case where the Nth CA certificate becomes is revoked (*pars. 0007, 0011-0012, and 0014-0020; Fig. 8; certificates 804 and 805 issued by CA 801 and CA 803 respectively are stored in hard disk of the computer 100*); and

an output unit operable to output, to a communication apparatus, the (N+1)th CA information stored in the CA information storage unit, the communication apparatus being connected to the (N+ 1)th download server via the communication network (*pars. 0007, 0011-0012, and 0014-0020; Fig. 8*), and

wherein said method comprises:
starting up the Nth authentication apparatus to place the Nth authentication apparatus in operation to issue the Nth server certificate (*pars. 0007, 0010-0014 and 0017-0020; Figs. 4-9*);

issuing, via the N^{th} CA information issue unit of the N^{th} authentication apparatus, the N^{th} CA information including (i) the N^{th} CA certificate indicating that the N^{th} server certificate is valid and (ii) the $(N+1)^{\text{th}}$ address for update indicating the location of the $(N+1)^{\text{th}}$ download server on the communication network (*pars. 0010- 0014, and 0017-0220; Fig. 4; certification authority address information 402; when the renewal program 102 of a certificate is started, according to the certificate authority address information 402 of the certificate 101, it will take connection 505 for the certificate authority 105 via a network*);

Kenichi does not explicitly disclose after said starting up of the operation of the N^{th} authentication apparatus, starting up the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server to place the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server into operation, said starting up of the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server taking place before a validity period of the N^{th} CA certificate expires; and terminating the operation of the $(N+1)^{\text{th}}$ download server after the validity period of the N^{th} CA certificate expires.

However, in an analogous art, Perlman discloses an authentication system, wherein after said starting up of the operation of the N^{th} authentication apparatus, starting up the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server to place the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server into operation, said starting up of the $(N+1)^{\text{th}}$ authentication apparatus and the $(N+1)^{\text{th}}$ download server taking place before a validity period of the N^{th} CA certificate expires (*Perlman: col. 3; lines 35-53; col. 7, lines 46-67 to col. 8, lines 1-24; begin using a new CA and OLRS, each of which*

have new respective private/public key pairs that are different from those used by the CA and OLRS that are no longer being used); and

terminating the operation of the (N+1)th download server after the validity period of the Nth CA certificate expires (Perlman: col. 3, lines 35-53; col. 7, lines 46-67 to col. 8, lines 1-24; if the CA is treated as if it has been compromised, in order to re-establish authentication system security it becomes necessary to (1) discontinue use of the current CA and OLRS, (2) begin using a new CA and OLRS, each of which have new respective private/public key pairs that are different from those used by the CA and OLRS that are no longer being used).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Perlman with the method and system of Kenichi to include steps of after said starting up of the operation of the Nth authentication apparatus, starting up the (N+ 1)th authentication apparatus and the (N+ 1)th download server to place the (N+1)th authentication apparatus and the (N+1)th download server into operation, said starting up of the (N+ 1)th authentication apparatus and the (N+ 1)th download server taking place before a validity period of the Nth CA certificate expires; and terminating the operation of the (N+1)th download server after the validity period of the Nth CA certificate expires to provide user with an authentication method that able to re-establish authentication system security after compromise of security information (Perlman: col. 1, lines 5-10).

- **Regarding claim 14,** Kenichi and Perlman disclose the method according to

Claim 13.

Perlman further discloses in said starting up of the $(N+1)^{th}$ download server, the $(N+1)^{th}$ authentication apparatus and the $(N+1)^{th}$ download server are put in operation, when the N^{th} CA certificate is revoked (*Perlman: col. 3; lines 35-53; col. 7, lines 46-67 to col. 8, lines 1-24; begin using a new CA and OLRS, each of which have new respective private/public key pairs that are different from those used by the CA and OLRS that are no longer being used*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Perlman with the method and system of Kenichi to include steps of in said starting up of the $(N+1)^{th}$ download server, the $(N+1)^{th}$ authentication apparatus and the $(N+1)^{th}$ download server are put in operation, when the N^{th} CA certificate is revoked to provide user with an authentication method that able to re-establish authentication system security after compromise of security information (*Perlman: col. 1, lines 5-10*)..

- **Regarding claim 15,** Kenichi and Perlman disclose the method according to

Claim 13.

Perlman further discloses terminating the operation of the N^{th} authentication apparatus and the operation of the $(N+1)^{th}$ download server when the validity period of the N^{th} CA certificate expires (*Perlman: col. 3, lines 35-53; col. 7, lines 46-67 to col. 8, lines 1-24; if the CA is treated as if it has been compromised, in order to re-establish*

authentication system security it becomes necessary to (1) discontinue use of the current CA and OLRS, (2) begin using a new CA and OLRS, each of which have new respective private/public key pairs that are different from those used by the CA and OLRS that are no longer being used).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Perlman with the method and system of Kenichi to include steps of terminating the operation of the Nth authentication apparatus and the operation of the (N+ 1)th download server when the validity period of the Nth CA certificate expires to provide user with an authentication method that able to re-establish authentication system security after compromise of security information (Perlman: col. 1, lines 5-10).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437